What is claimed is:

1. A method of signing and authenticating electronic documents comprising:

securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster;

receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user;

identifying the signing request as one transmitted by the first user, and identifying a signature ready document to be signed;

retrieving at the local computer cluster a private key portion associated with the first user from the private key database

generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key;

retrieving at the local computer cluster the signature ready document to be signed; and

signing the signature ready document on the local computer cluster using the generated complete private key to produce a signed document.

2. The method of claim 1 wherein the private key portion is a complete private key.

3. The method of claim 1 wherein generating a complete private key using the retrieved private key portion includes:

receiving signing identification credentials from the first user; and constructing a complete private key using the private key portion and the received signing identification credentials.

4. The method of claim 1 wherein the received signing request was transmitted from the first remote computer to the local computer cluster over the internet.

5. The method of claim 1 wherein the received signing request was transmitted from the first remote computer to the local computer cluster over the world wide web using a hypertext transport protocol, and wherein the signing request was transmitted using a browser running on the remote computer.

6. The method of claim 5 wherein the retrieving at the local computer cluster the signature ready document is automatic.

7. The method of claim 5 wherein the retrieved signature ready document is a standard generalized markup language document.

8. The method of claim 1 further comprising storing the signature ready document in a first document database.

9. The method of claim 8 further comprising prior to signing:

receiving form data from the first remote computer; and modifying the retrieved signature ready document based on the received form data.

10. The method of claim 8 wherein the first document database is located on the local cluster.

11. The method of claim 8 wherein the first document database is located on a secure second remote computer.

12. The method of claim 8 further comprising storing the signed document in a second document database.

13. The method of claim 12 wherein the second database is located on a secure second computer remote computer.

14. The method of claim 12 wherein the second database is located on the local computer cluster.

15. The method of claim 12 further comprising associating at least one of the signature ready document and the signed document with a document owner.

16. The method of claim 15 further comprising notifying at least one of document owner and the first user that a signature ready document or a signed document has been signed.

17. The method of claim 1 further comprising registering individuals as users, wherein registering includes:

verifying and recording the identity of individuals registering;

digitizing and recording handwritten signatures of individuals registering;

associating passwords with the recorded digitized handwritten signatures and the recorded identities; and

storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster.

18. The method of claim 17 further comprising:

recording biometric measurements of individuals registering;

associating the biometric measurements of individuals registering with the recorded identities of the individuals registering; and

storing the biometric measurements in the identity database.

19. The method of claim 18 further comprising detecting using the biometric measurements whether individuals have previously registered.

20. The method of claim 17 wherein the first user is a registered user.

21. The method of claim 20 wherein the signing comprises:

a) appending the first user's digitized signature to the signature ready document;

b) making a hash of the signature ready document; and

c) encrypting the hash of the signature ready document with the first user's private key.

22. The method of claim 17 further comprising:

associating and storing a secret set of recognition graphics with the passwords in the identity database;

displaying a plurality of recognition graphics, including recognition graphics from the secret set, on the first remote computer;

requesting the first user to select graphics included in the secret set using a non-keyboard selecting device attached to the first remote computer;

receiving a message from the first remote computer identifying the selected graphics;

authorizing access to the local computer cluster if the selected graphics are included in the secret set.

23. The method of claim 17 further comprising:

generating the private key portions for individuals registering, wherein the private key portions can be used with signing identification credentials to construct complete private keys;

associating the generated private key portions with the recorded identities of individuals registering

storing private key portions in a private key database.

24. A method of signing and authenticating electronic documents comprising:

running a browser on a first remote computer;

connecting to a local computer cluster via a computer network using the browser;

transmitting user identification information and document identification information to the local computer cluster;

transmitting a signing request to the local computer cluster, the signing request requesting the local computer cluster to retrieve the identified document from a second remote computer, to obtain a private encryption key associated with the identified user from a third remote computer, and to sign the retrieved document using the obtained private key on a fourth computer, wherein the first, second, third, and fourth remote computers can be the same computer or different computers.

25. A system for signing and authenticating documents comprising local computer cluster, the local computer cluster including:

a first memory device having a first program stored thereon; and a first processor coupled to the first memory, wherein the first processor can read the first program stored in the first memory and can perform the steps of:

securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster;

receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user;

identifying the signing request as one transmitted by the first user, and identifying a signature ready document to be signed;

retrieving at the local computer cluster a private key portion associated with the first user from the private key database

generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key;

retrieving at the local computer cluster the signature ready document to be signed; and

signing the signature ready document on the local computer cluster using the generated complete private key to produce a signed document.

26. The system of claim 25 further comprising a second remote memory device having stored thereon a signature ready document database, wherein the second memory device is remotely connected to the local computer cluster.

27. The system of claim 25 wherein the local computer cluster further comprises a second memory device having stored thereon a signature ready document database, wherein the second memory device is coupled to the processor.

28. The system of claim 25 further comprising a second memory device having stored thereon a signed document database, wherein the second memory device is remotely connected to the local computer cluster.

29. The system of claim 25 wherein the local computer cluster further comprises a second memory device having stored thereon a signed document database, wherein the third memory device is coupled to the processor.

30. The system of claim 25 wherein the local computer cluster further comprises a second memory device having stored thereon an identity database, the identity database including user digitized handwritten signatures, recorded user identities associated with the signatures, and passwords associated with the user identities.

31. The system of claim 25 wherein the processor can perform the additional steps of:

receiving form data from the first remote computer; and

modifying the retrieved signature ready document based on the received form data.

32. The system of claim 25 wherein the received signature ready document is a standard generalized markup language document.

33. The system of claim 25 wherein the retrieving at the local computer cluster the signature ready document is automatic.

34. The system of claim 25 further comprising a registration computer connected to the local computer cluster.

35. The system of claim 34 wherein the registration computer comprises a second memory device having a second program stored thereon; and

a second processor coupled to the second memory, wherein the second processor can read the second program stored in the second memory and can perform the steps of:

recording the identity of individuals registering;

and recording digitized handwritten signatures of individuals registering;

associating passwords with the recorded digitized handwritten signatures and the recorded identities; and

storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster.

36. A system for signing and authenticating documents comprising:

a means for securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster;

a means for receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user;

a means for identifying the signing request as one transmitted by the first user, and identifying a signature ready document to be signed;

a means for retrieving at the local computer cluster a private key portion associated with the first user from the private key database

a means for generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key;

a means for retrieving at the local computer cluster the signature ready document to be signed; and

a means for signing the signature ready document on the local computer cluster using the generated complete private key to produce a signed document.

37. The system of claim 36 further comprising a means for storing the signature ready document in a first document database.

38. The system of claim 37 further comprising a means for storing the signed document in a second document database.

39. The system of claim 38 further comprising a means for associating at least one of the signature ready document and the signed document with a document owner.

40. The system of claim 39 further comprising a means for notifying at least one of document owner and the first user that a signature ready document or a signed document has been signed.

41. The system of claim 36 further comprising a means for registering individuals as users, wherein the means for registering includes:

a means for verifying and recording the identity of individuals registering;

a means for digitizing and recording handwritten signatures of individuals registering;

a means for associating passwords with the recorded digitized handwritten signatures and the recorded identities; and

a means for storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster.

42. The system of claim 41 further comprising:

a means for recording biometric measurements of individuals registering;

a means for associating the biometric measurements of individuals registering with the recorded identities of the individuals registering; and

a means for storing the biometric measurements in the identity database.

43. The system of claim 42 further comprising a means of detecting using the biometric measurements whether individuals have previously registered.

44. The system of claim 36 wherein the first user is a registered user.

45. The system of claim 44 wherein the means of signing comprises:

a) a means of appending the first user's digitized signature to the signature ready document;

b) a means of making a hash of the signature ready document; and

c) a means of encrypting the hash of the signature ready document with the first user's complete private key.